IPv6 over Link-Local Discovery Protocol

draft-richardson-anima-ipv6-lldp

M. Richardson
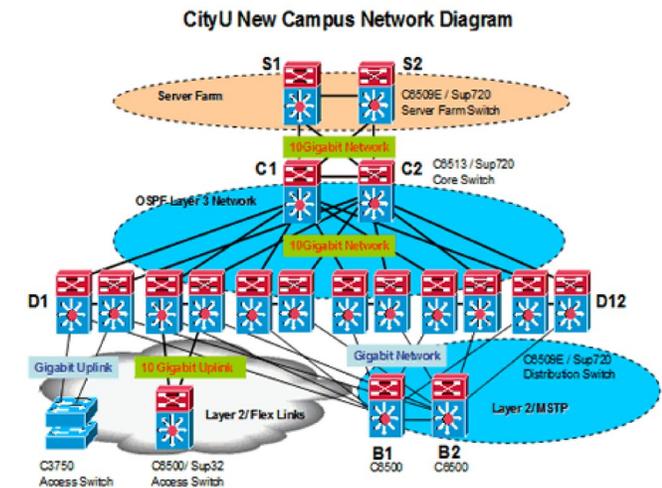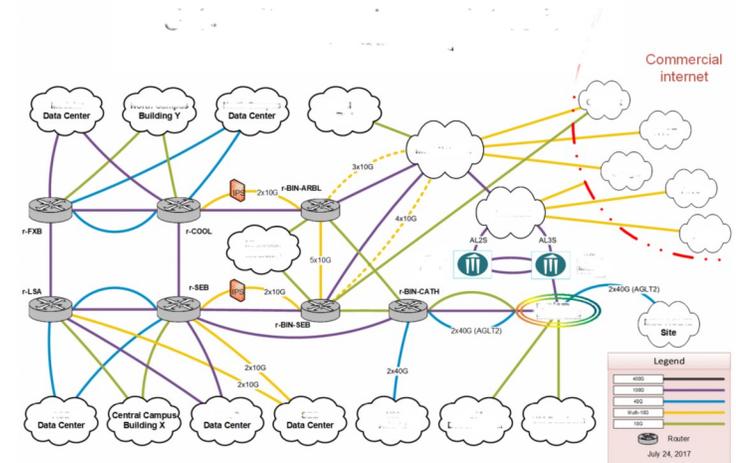
Liang Xia

Jie Yang(presenting)

IETF 107, ANIMA

Challenges in creating
Autonomic Control Plane (ACP) in
Layer-2 Software Defined Networks (SDN)

SDN managed Layer-2 networks have multiple, redundant links between routers.

CityU New Campus Network Diagram

Booting SDN depends upon ACP

- Stable SDN connection can provided by RFC8368.
  - (RFC8368 : Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM))
- But before the connection, Broadcast in this Campus L2 systems, => Loop
  - Need additional mechanism for Loop-breaking
  - Like STP …
    - But can't automatically configure during on-boarding process
    - May miss some devices
    - May discover untrusted devices!
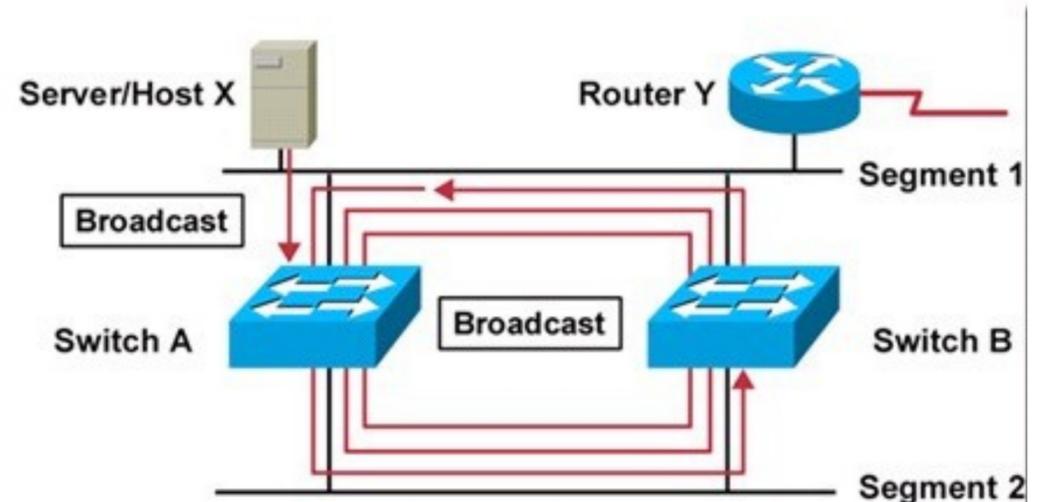
Background on LLDP

- LLDP *(Link Layer Discovery Protocol)*

Description:

- Standard Layer-2 discovery protocol in IEEE 802.1ab, without Control Plane
- **Does not forward packets!**
  - that is : it discovers all compliant layer-2 devices in a network, even if they do not normally do any layer-3 processing
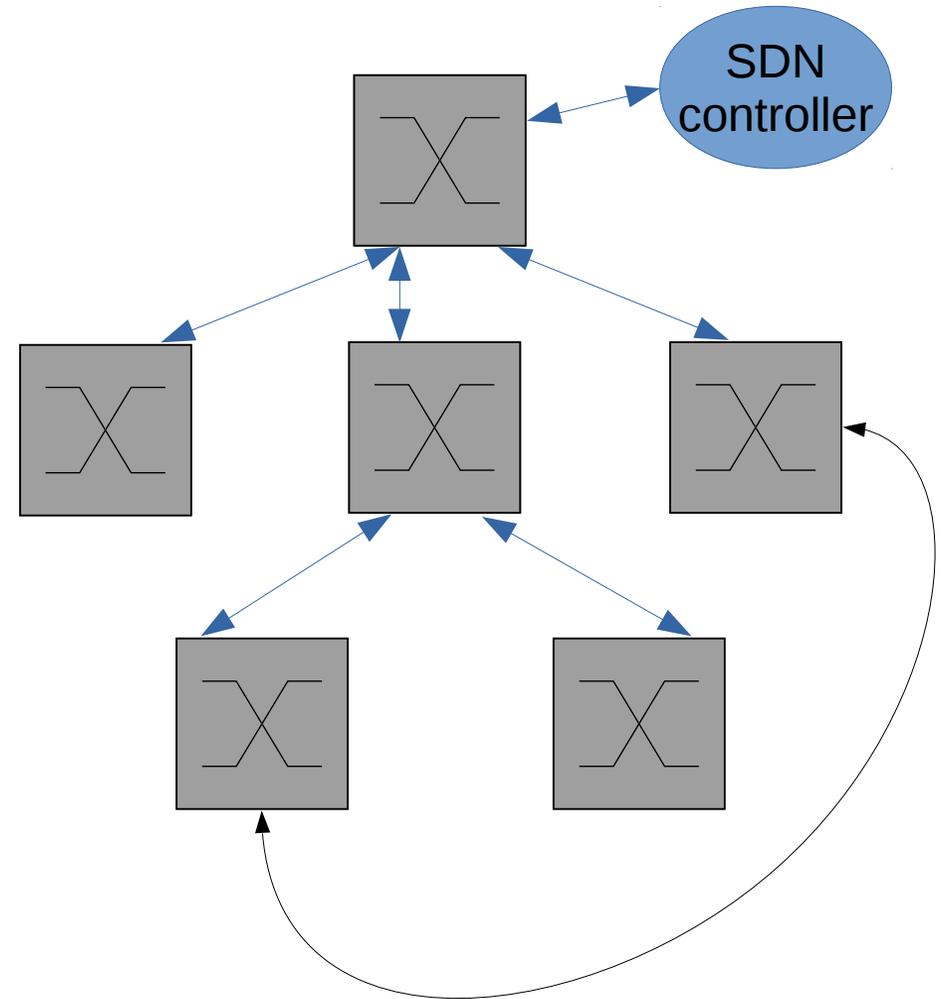- No forwarding, means no loops

About LLDP frames:

- Forwarding plane already sends LLDP to control plane CPU.
  - exactly the desired behaviour for ACP: all traffic goes to the control plane processor!
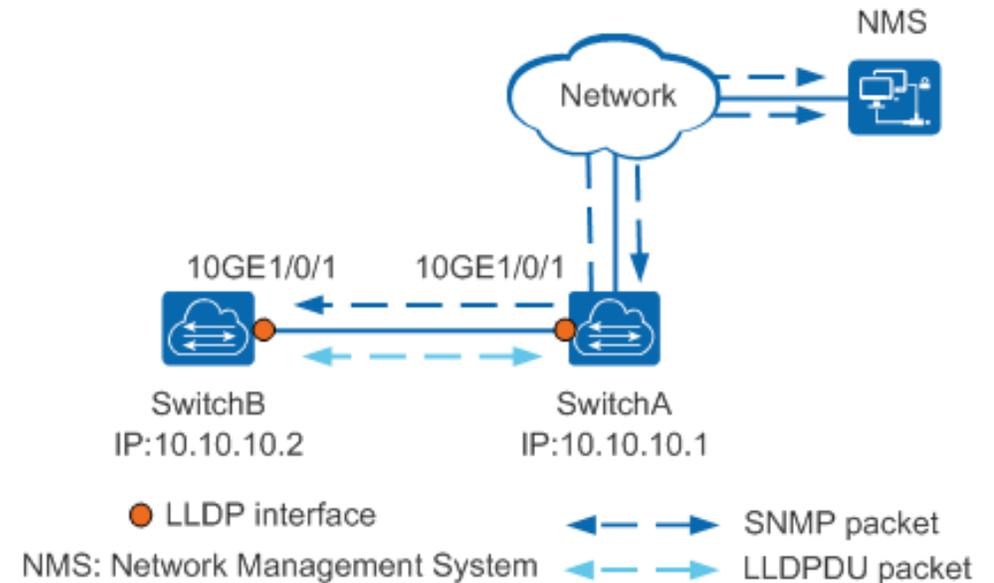
Other needs for SDN based Layer 2

- Must discover every legitimate switch
  - Through multiple layers of L2 connectivity
- Must avoid including end systems (desktops, compute servers) into topology
  - Malware on such systems could pretend to be a router
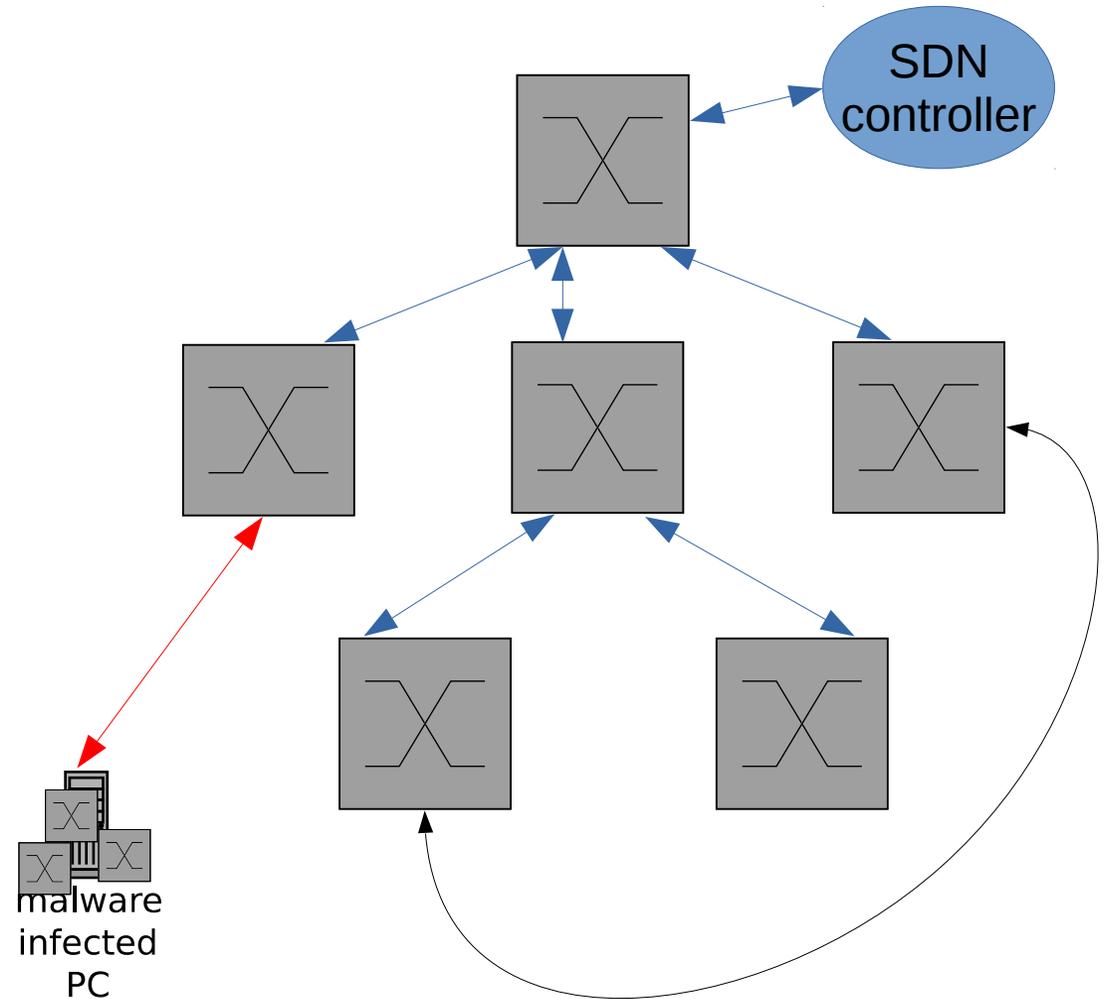- Discovery must run at power on, and continously whenever a link change occurs

Other needs for SDN based Layer 2

- Must discover every legitimate switch
  - Through multiple layers of L2 connectivity
- Must avoid including end systems (desktops, compute servers) into topology
  - Malware on such systems could pretend to be a router
- Discovery must run at power on, and continously whenever a link change occurs
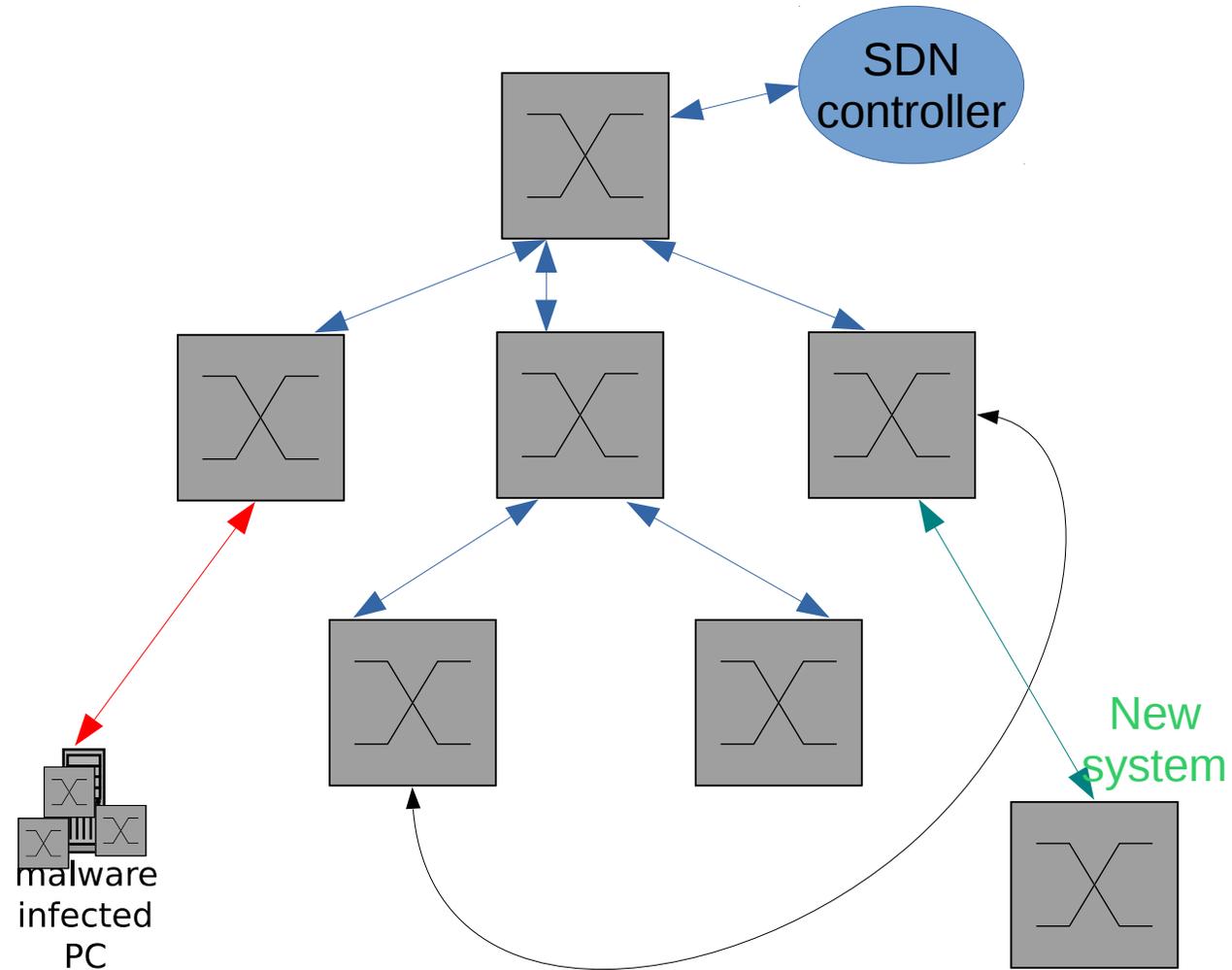
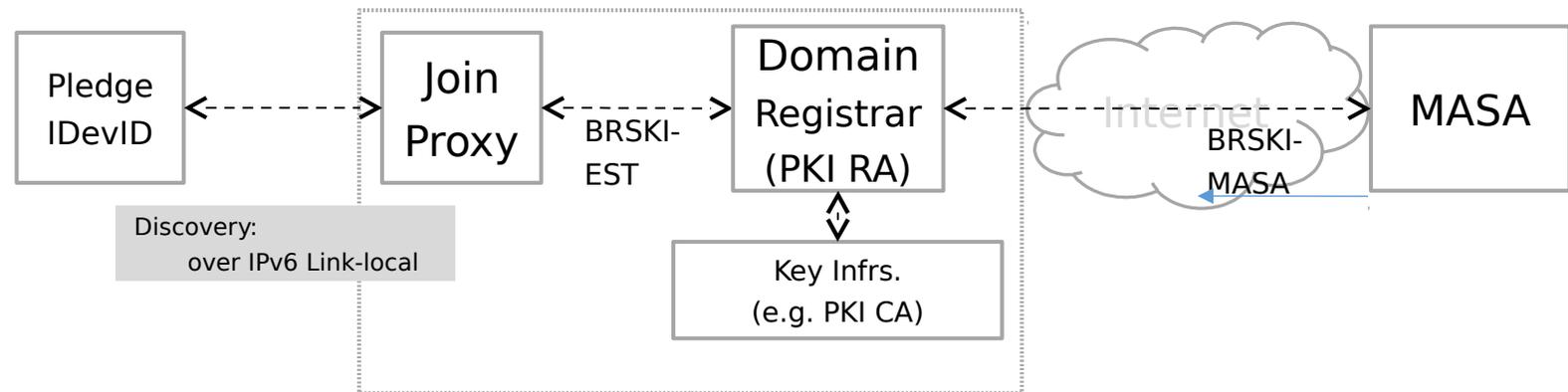SDN controller

malware infected PC

Other needs for SDN based Layer 2

- Must discover every legitimate switch
  - Through multiple layers of L2 connectivity
- Must avoid including end systems (desktops, compute servers) into topology
  - Malware on such systems could pretend to be a router
- Discovery must run at power on, and continously whenever a link change occurs

Do all discovery with ACP inside LLDP

- Encapsulate IPv6 in LLDP's Type-Value-Length (TLV) system

- Build ACP using LLDP packets, which authenticates each end

- ACP adjacency table, becomes adjcancy table for L2

- Onboard new switches using BRSKI, with Join Proxy help.

LLDP Protocol Encapsulation and issues
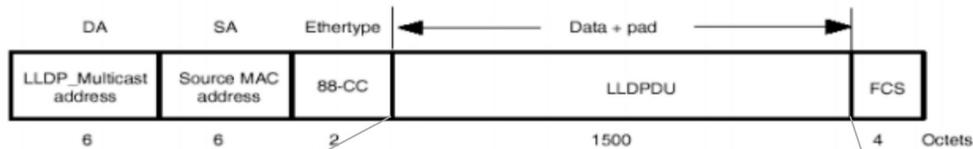

LLDP Frame Formats

DA	SA	Ethertype		Data + pad	
LLDP_Multicast address	Source MAC address	88-CC		LLDPDU	FCS
6	6	2		1500	4 Octets

Figure D-1—IEEE 802.3 LLDP frame format

Extension TLV type 111 1111	TLV string length	Organizationally unique identifier (OUI)	Group-defined TLV subtype	Group-defined information string
7 bits	9 bits	3 octets	1 octet	$0 \le n \le 507$ octets

TLV header → TLV information string 4 - 511 octets
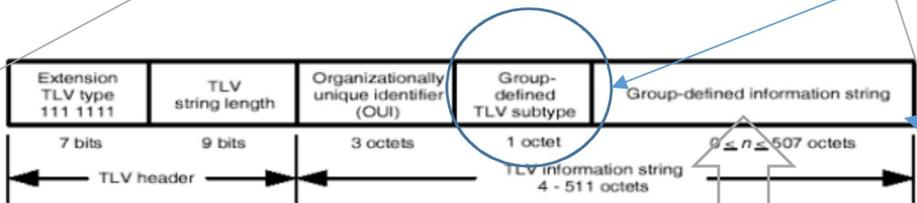
Figure 9-12—Basic format for organizationally-defined extension TLVs

Vendor-specific TLV : 127	IANA unique	TBD	IPv6 fragment : up to 507 octets

- About 508 octets limit of vendor-specific frame:
  - And the minimum MTU in IPv6 protocol : 1280
  - So LLDP IPv6 fragment contain **more than one** TLV, accommodate up to 1500bytes(often larger…) in Ethernet network

LLDP issues

Issue of Subtype TLV values: which better?

Option-1: Multiple different subtype values

Option-2: Repeatedly same subtype TLV values

How to keep the correct order?

Issue of Content payload : which option?

Option-1: entire IPv6 packet

Option-2: elided IPv6 packet

Option-3: compressed packet, RFC8138 or others?

Thank You!